

1. SAYI
OCAK - ŞUBAT 2024

DİJİTAL BÜLTEN

MAKALE

- Sızma Testleri ve Ceza Hukuku
- Sosyal Ağ Sağlayıcılarının Hukuki Sorumluluğu
- Dijital Hizmetler Yasası Uyum Sürecine İlişkin Gelişmeler
- Avrupa Birliği Veri Yasası

İNFOGRAFİK

- Phishing Saldırısı nedir? Nasıl Korunuruz?



İstanbul Barosu

Bilişim Hukuku Komisyonu

İçindekiler

Makaleler

Kısa Kısa	03
Sızma Testleri ve Ceza Hukuku	07
Sosyal Ağ Sağlayıcılarının Hukuki Sorumluluğu	11
Dijital Hizmetler Yasası Uyum Sürecine İlişkin Gelişmeler	18
Avrupa Birliği Veri Yasası	20

İnfografik

Phishing Saldırısı	25
--------------------	----



KISA KISA

Av. Pınar Saruhan & Av. Mert Özyiğit

Finlandiya Ekosistemi Tarafından Başlatılan Metaverse Girişimi: Sanal Potansiyelden Gerçek Dünya Etkisine

Finlandiya, yayınladığı raporunda 2035 yılına kadar Metaverse’de küresel bir lider olmak istediğini duyurdu. Rapor; Avrupa Birliği (“AB”) ülkelerinden gelen ilk ulusal Metaverse stratejisi olduğundan 2035 yılına kadar Birleşmiş Milletler’in(“BM”) Sürdürülebilir Kalkınma Hedeflerini tamamlaması, vatandaşların teknoloji ile tanışması ve bu konuda eğitilmesi gibi hedefler de yer arıyor.

Detaylı bilgi için: [tıklayın.](#)



Avrupa Birliği’nden Dijital Kimlik Cüzdanı

İnsanların ve şirketlerin güvenli ve güvenilir elektronik kimlikler ve doğrulamalara ulaşımını amaçlayan düzenleme olan Avrupa Birliği Dijital Kimlik Cüzdanı kapsamında, AB üyesi ülkeler, vatandaşlara ve şirketlere dijital kimlik cüzdanı kullanma olanağı sunmaktadır.

Bahse konu dijital kimlik cüzdanları Avrupa genelinde tanınarak, kişisel verilerin amaç dışında paylaşımının da önüne geçmiş olacaktır. Gerekli teknik çalışmalar tamamlandıktan sonra ilgili düzenleme AB’ye üye devletlerin onayına tabi tutulacaktır.

Detaylı bilgi için: [tıklayın.](#)

KISA KISA



Singapur Siber Güvenlik Tedbiri

Singapur Sağlık Bakanlığı, Singapur Siber Güvenlik Ajansı ile iş birliği içinde, sağlık hizmeti sağlayıcıları için özel olarak hazırlanmış siber güvenlik yönergelerini yayımlamıştır. Bu yönergeler, hassas bilgileri içeren bir ihlal durumunda verilerin uygun şekilde güvence altına alınmasının, güncel yazılımların sürdürülmesinin ve stratejik bir müdahale planının formüle edilmesinin kritik önemini altını çizmektedir. Singapur Sağlık Bakanlığı ayrıca sağlık bilgilerinin güvenli bir şekilde toplanmasını, erişilmesini, kullanılmasını ve paylaşılmasını düzenlemek amacıyla 2024 yılında Sağlık Bilgi Yasası'nı çıkarmaya hazırlanmaktadır.

Detaylı bilgi için: [tıklayın.](#)

Avrupa Siber Güvenlik Dayanışma Yasası

Avrupa Parlamentosu("AP") Sanayi, Araştırma ve Enerji Komitesi (Industry, Research and Energy Committee) Avrupa Siber Güvenlik Dayanışma Yasası (Cyber Solidarity Act) ("Yasa") taslak raporunu kabul etti. Yasa, büyük ölçekli gerçekleşen siber saldırılara karşı AB'nin siber dayanıklılık kapasitesini arttırmayı, siber saldırıları tespit etmek ve iş birliğini artırmanın yanı sıra, Avrupa Siber Güvenlik Kalkanı oluşturmayı da hedeflemektedir. Rapor, özellikle tehdit bilgisi paylaşımının kolaylaştırılması yoluyla siber güvenlik risklerini azaltmak için tasarlanmış değişiklikler, bütçe hususları ve stratejik girişimler içermektedir. AP, 2024 yılında AB kurumları arasında kurumlar arası müzakereleri öngörerek bu siber güvenlik tedbirlerini resmileştirmeyi ve uygulamayı amaçlamaktadır.

Detaylı bilgi için: [tıklayın.](#)



KISA KISA



Sosyal medya bağımlılığının önlenmesine ilişkin yasa tasarısı

AP tarafından sosyal medya bağımlılığının önlenmesine ilişkin yasa tasarısı ("Tasarı") kabul edilmiştir. Onaylanan Tasarı içerisinde, bağımlılık yaratan tekniklerin (örneğin sonsuz kaydırma veya otomatik oynatma) yasaklanması, dikkat ekonomisinden etik tasarıma geçiş, dijital "rahatsız edilmeme hakkı"nın tanıtılması ve tüm internet hizmet ve ürünlerinin çocuklar için güvenli hale getirilmesi gibi önlemler bulunmaktadır. AP'nin onayladığı bu Tasarı, sosyal medya uygulamaları ve çevrimiçi satış oyun sitelerinin bağımlılık yaratıcı özelliklerini azaltmayı ve tüketicileri korumayı hedeflemektedir.

Detaylı bilgi için: [tıklayın.](#)

Dijital Türk Lirası

Türkiye Cumhuriyeti Merkez Bankası, 'Dijital Türk Lirası' projesinde birinci faz değerlendirme raporunu yayınladı.

Raporda genel olarak Dijital Paranın tanımı, temel gereksinimleri ve uygulaması üzerinde duruldu.

Detaylı bilgi için: [tıklayın.](#)

Blockchain Tabanlı Hizmet Ağı

Çin Kamu Güvenliği Bakanlığı, Blockchain Tabanlı Hizmet Ağı'nın ("BTHA") desteğiyle gerçekleştirilen RealDID girişimini duyurmuştur. Çin'in ulusal çapta bir Blockchain girişimi olan BTHA yaptığı bir duyuruyla Blockchain teknolojisinin, Çin'deki 1,4 milyar nüfusun gerçek isim kimliklerini doğrulamak için kullanılacağını açıklamıştır. RealDID hizmeti, kullanıcıların DID adreslerini ve özel anahtarları kullanarak web sitelerine anonim olarak kaydolmalarına ve oturum açmalarına olanak tanıyarak iş verilerinin ve işlemlerin kişisel bilgilerle bağlantısının kesilmesine imkân sağlayacaktır.

Detaylı bilgi için: [tıklayın.](#)

KISA KISA



Yayın Kuruluşlarına Düzenleme

İnternet ortamından yayın yapan kuruluşların lisans ve yetkilendirme süreçlerine ilişkin bazı önemli düzenlemeler 13 Ocak 2024'te Resmî Gazete'de yayımlandı. İnternet ortamında yayın yapan kuruluşların kurumsal internet sitelerinde künye, iletişim ve adres bilgilerini, sorumlu müdürün adı soyadını ve iletişim bilgilerini, tebligat adresini, yayın hizmetinin iletiği platformlar ile kurumsal internet sitesi haricindeki internet sitelerini bulundurması zorunlu hale getirilirken İnternet ortamından yayın lisansı almak üzere başvuran kuruluşların yayın lisans ücretini ödemeleri zorunlu hale getirildi. Yönetmelikler, yayımlandıkları tarihte yürürlüğe girdi.

Detaylı bilgi için: [tıklayın.](#)

AYM'den İptal Kararı

Anayasa Mahkemesi'nin (" AYM ") 2020/76 E., 2023/172 K. sayılı kararı ("Karar") ile 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un ("5651 sayılı Kanun") bazı hükümleri Anayasa'ya aykırı bulunarak iptal edildi. 5651 sayılı Kanun'un kişilik haklarını ihlal eden internet yayınlarına erişimin engellenmesi veya içeriğin çıkarılması işlemlerine ilişkin usul ve esasların düzenlendiği 9 madde tamamen, Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından erişimin engellenmesi dışında içeriğin yayından çıkarılması kararı verilmesini ve BTK tarafından erişim sağlayıcılar yanında içerik ve yer sağlayıcılara idari para cezası verilmesini düzenleyen 8 madde ise kısmen iptal edildi. Karar'ın tamamında yer alan iptal hükümleri 10 Ekim 2024 tarihinde yürürlüğe girecektir.

Detaylı bilgi için: [tıklayın.](#)

— *Av. Celil Aktaş*

Sızma Testleri ve Ceza Hukuku

Sızma Testi Nedir? Sızma
Testleri'nin Türk Ceza
Kanunu Yansımaları

- Giriş

Bilişim sistemlerinin hayatın her alanında merkezi bir rol üstlenmesiyle bu sistemlerin olası saldırılardan korunmaları, hiç olmadığı kadar önemli olmuştur. Bir bilişim sisteminin herhangi bir saldırıya karşı dayanıklı olup olmadığının anlaşılmasında sızma (penetrasyon) testlerinin en etkili araçlardan olduğu şüphesizdir.

Ancak bu testler yapılırken yasal sınırların aşılmaması gerekmektedir zira aksi halde cezai sorumluluğun söz konusu olacağı açıktır.

Sızma Testi Nedir?

Sızma testleri, bir bilişim sisteminin açıklarını ortaya çıkarmak maksadıyla gerçekleştirilen siber saldırılardır¹. Bu testler, bir bilişim sisteminin zafiyetlerini, bunlar başka kişilerce tespit edilmeden önce tespit edilip giderilebilmeleri amacıyla yapılırlar.

Bu sayede, söz konusu bilişim sisteminde bilgi güvenliği esaslı şekilde gerçekleştirilebilir².

Sızma testleri, bu testleri uygulayacak olan taraf ile testin uygulanacağı bilişim sisteminin sahipleri arasında düzenlenen sözleşmeler çerçevesinde gerçekleştirilirler. Bu sözleşmeler, sızma testinin kapsamı, niteliği, sonuçların raporlanması ve gizlilik gibi çeşitli hususları düzenleyen hükümler içerirler. Ancak söz konusu sözleşmelerin içerikleri ne olursa olsun sızma testi uygulayıcılarının sözleşmeyle çizilen sınırı, kesin olarak aşmamaları gerekir. Zira, hareketlerinin hukuka aykırılığını ortadan kaldıran husus, bu sözleşmelerdir. Öte yandan sızma testlerinin uygulanması ticari sırların ele geçirilmesi, haksız rekabetin ortaya çıkması, kişisel verilerin ele geçirilmesi gibi konularda hukuki ve cezai anlamda sorumluluklar getirmektedir. Bu yazıda cezai yükümlülüklerin ve yaptırımların üzerinde durulacaktır.

Sızma Testleri'nin Türk Ceza Kanunu Yansımaları

5237 sayılı Türk Ceza Kanunu'nda ("TCK") tanımlanan suçlardan bazıları, sızma testleri açısından öne çıkmaktadır. Bu konuda sınırlandırma yapmak mümkün gözükmemekle beraber öne çıkabilecek başlıca TCK hükümleri m. 243, m. 244, m. 136 ve m. 137 hükümleridir.

- Bilişim Sistemine Girme Suçu (TCK m. 243)

TCK'nin 243. maddesinde düzenlenen bilişim sistemine girme suçu, failin bir bilişim sisteminin tamamına veya bir kısmına hukuka aykırı şekilde kasten girmesi veya orada kalmaya devam etmesiyle oluşur. TCK m. 243 hükmünün lafzında sızma hareketinin hukuka aykırı şekilde gerçekleşmesinin aranması önemlidir. Çünkü söz konusu suç açısından hukuka aykırılık, tipikliğin oluşması için zorunludur.

Bir bilişim sistemine söz konusu sistemin sahibinin rızası veya hukuken geçerli bir sözleşme çerçevesinde girilmesi halinde, bilişim sistemine girme suçu sübut bulmaz.



O halde, sızma testleri çerçevesinde bilişim sistemine girilmesi ve burada kalınması eylemleri bir sözleşme kapsamında yapıldığı için hukuka aykırı olmayacaktır. Başka bir ifadeyle bu suçun unsurları sözleşmedeki sınırlara uyuldukça ortaya çıkmamakla birlikte sözleşme çerçevesi dışına çıktığında bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam etme eylemleri olarak suçun fiil unsurları oluşabilmektedir. Söz gelimi, sözleşmede bir bilişim sisteminin sadece bir kısmı için sızma testi uygulanması öngörülmüş ancak uygulayıcılar, sistemin tamamına test kapsamında girmişlerse bu durumda bilişim sistemine girme suçu sübuta ermiş olarak değerlendirilebilir.

- Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)

Sızma testlerinde konu, her zaman bir sisteme girilmesi olmayabilir. Örneğin, bu testler kapsamında bir DDoS (Dağıtık Hizmet Engelleme) saldırısı gerçekleştirilirse, sistemin engellenmesi söz konusu olacaktır. Çünkü sistemin engellenmesi, bir bilişim sisteminin işlevlerini yerine getirmesinin önüne geçilmesi veya kısıtlanması ya da sistemin yavaşlatılması anlamına gelir. O halde bir sızma testi kapsamında bir bilişim sistemine erişiminin engellenmesi, kısıtlanması veya yavaşlatılması hallerinde bu suçun tipik unsurları oluşacaktır.

Bilişim sistemine yönelik engellemeler, ilgililerin rızası ve bilgisi dahilinde yapılmışsa TCK'nin 244. maddesinde tanımlı suç sübut bulmayacaktır. Ancak verilen rızanın aşıldığı hallerde söz konusu suçun sübut bulacaktır. Bu nedenle sızma testi sözleşmesi, bu kez hukuka aykırılığı ortadan kaldıran hallerden "ilgilinin rızası" (TCK m. 26) çerçevesinde öne çıkacaktır. Zira, söz konusu sözleşmeler, sızma testinin uygulayıcıları ile testin uygulandığı bilişim sisteminin sahibi gerçek veya tüzel kişi arasında düzenlenmektedirler. Bundan dolayı bu sözleşmelerin varlığı, hukuka aykırılığı ortadan kaldıran hallerden kabul edilmelidir. Hal böyle olunca, suçun tipik unsurları oluşsa bile hukuka aykırılık unsuru oluşmadığından sözleşmeye uygun şekilde uygulanan bir sızma testi kapsamında TCK'nin 244. maddesinde tanımlı suçun sübut bulmayacağı kanaati ağır basmaktadır.

- Verileri Ele Geçirme veya Yayma Suçu (TCK m. 136)

Günümüzde bankacılık ve e-ticaret sektörü başta olmak üzere dijital alanlarda saklanan kişisel veriler çeşitli sorumluluklar gerektirmektedir. Sızma testleri; bir siber güvenlik amacıyla teknik tedbir olarak da uygulanmaktadır. Bu noktada sızma testlerinde sisteme erişen uygulayıcılar, sistemde kişisel veri niteliğini haiz verilere erişme fırsatı elde edebilirler. Böyle bir durumda sızma testi uygulayıcılarının bu verileri ele geçirmeleri veya yaymaları halinde TCK'nin 136. maddesinde tanımlı verileri ele geçirme veya yayma suçunun işlenmiş olacağı izahtan varestedir. Nitekim, sızma testi sözleşmesi onlara böyle bir yetki vermeyeceğinden hareketleri hukuka aykırı olacaktır.

Bununla birlikte TCK m. 137/2 hükmünde düzenlenen nitelikli hal, konumuz açısından önem kazanmaktadır. Söz konusu hüküm uyarınca bu suç, bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenirse verilecek ceza yarı oranında artırılabilecektir. Bu nitelikli halin uygulanabilmesi için ilgili mesleki faaliyetlerle suçun işlenişi arasında nedensellik bağı bulunmalıdır.

Sızma testi uygulayıcılarının bir sızma testi sözleşmesinden kaynaklanan hak ve yükümlülüklerini kötüye kullanarak kişisel verilerin ele geçirilmesi veya yayılması suçunu işlemeleri de söz konusu nitelikli hal kapsamında değerlendirilmelidir. Çünkü fail, kişisel verilere bu testin icrası sırasında erişmekte ve bunları bu sayede ele geçirip yaymaktadır. Hal böyle olunca, sızma testinin sağladığı kolaylıktan yararlanarak bu suçu işleyen fail hakkında verilecek cezada artırımı gidilmelidir. Bununla birlikte, sızma testi uygulayıcıları özelinde TCK madde 239 hükmü de gündeme gelecektir. Nitekim bu madde ile sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgileri yetkisiz kişilere veren veya ifşa eden kişinin, üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılacağı belirtilmektedir.

Sonuç ve Değerlendirme

Günümüzde internetin hayatımızın vazgeçilmezi olması ve e-ticaret, bankacılık sektörleri dahil olmak üzere internet aracılığıyla hizmet alınan sektörler özelinde hukuka uygun bir sızma testinin yapılması gibi siber güvenlik önlemlerinin alınması gerekmektedir. Sızma testlerinin TCK hükümlerine uyum sağlanması kaydıyla; yetkisiz erişim, erişim sınırlarının aşılması, veri ihlali, verilerin hukuka aykırı olarak kullanılması gibi yasadışı faaliyetlerin önlenmesinin son derece önemli olduğu açıkça ortadadır.

Tüm bu nedenlerden dolayı sızma testini uygulayıcıları, aslında ince bir çizginin üzerinde yürümektedirler. Nitekim sızma testlerinde sözleşmenin düzenlenmesi gerekliliği yeterli olmamakta bu sözleşmede yer alan hükümlere uygun biçimde testlerin yapılması gerektiği yani çerçevenin kurallarının çizilerek çerçeve içerisinde kalınması son derece önemlidir. Sızma testinin uygulanması sırasında sözleşmede çizilen sınırlar aşılsa yukarıda ele aldığımız suçlar başta olmak üzere TCK'de tanımlı pek çok suça konu eylemin gerçekleşme riski yüksektir.

Bu nedenle sızma testi sözleşmeleri, özellikle bu testleri uygulayanlar açısından, sadece taraflar arası bir sözleşmeden ibaret görülmemeli, hukuka aykırılığı önleyen esaslar olarak kabul edilmelidir. Sonuç olarak cezai sorumluluklar da göz önünde bulundurularak sızma testi sözleşmesi düzenlenmeli ve ifa edilmelidir.





Av. Merve ASLAN

Sosyal Ağ Sağlayıcılarının Hukuki Sorumluluğu

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[1] (“İnternet Kanunu”); kamuoyunda “Yeni Sosyal Medya Yasası” olarak bilinen 7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun[2]; kamuoyunda

“Dezenformasyon Yasası” olarak bilinen 7418 sayılı “Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun[3]” ve Bilgi Teknolojileri ve İletişim Kurulu’nun (“BTK”) Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar başlıklı Kararı (“Karar”) ile sosyal ağ sağlayıcı olarak tanımlanan gerçek veya tüzel kişilerin yükümlülükleri belirlenmekte, bu yükümlülüklerin nasıl uygulanacağına dair usul ve esaslar detaylandırılmaktadır.

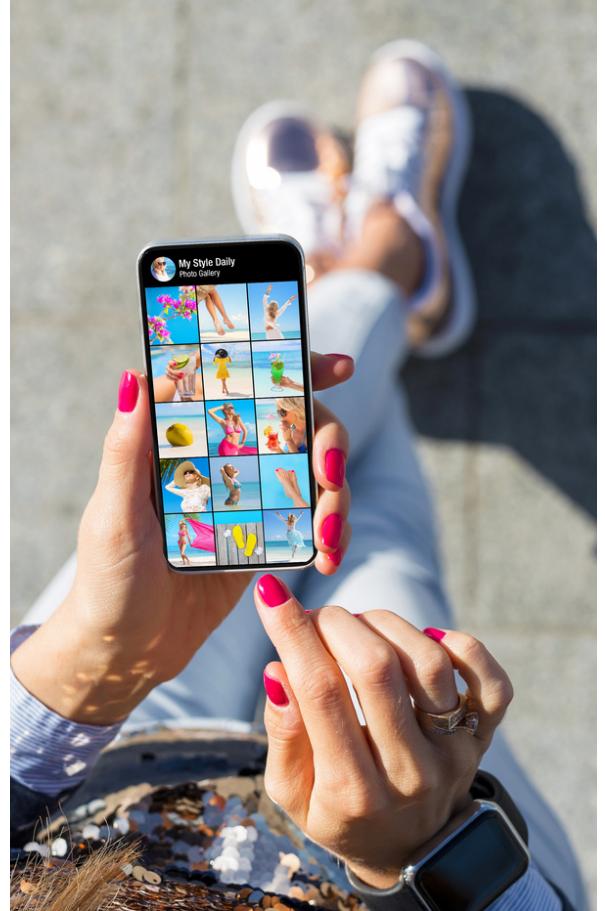
X (eski adıyla Twitter), Instagram, Facebook, TikTok, LinkedIn ve Youtube gibi sosyal ağ sağlayıcılar, kullanıcılarının sosyal etkileşim amacıyla internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek ve tüzel kişiler olarak tanımlanmaktadır. Sosyal etkileşim amaçlı içeriklerin asli amaç olmadığı, ikincil ve yan hizmet olarak sunulduğu, haber siteleri, e-ticaret siteleri ve kişisel internet siteleri gibi platformlar sosyal ağ sağlayıcı olarak değerlendirilmemekte ve dolayısıyla Karar kapsamı dışında bırakılmaktadır. Ayrıca belirtmek gerekir ki, Karar kapsamında belirlenen usul ve esasların uygulanması sosyal ağ sağlayıcının içerik ve/veya yer sağlayıcı olmasından doğan sorumluluk ve yükümlülüklerini ortadan kaldırmamaktadır.

Temsilci Atama ve Bildirme Yükümlülüğü

Günlük erişimi bir milyondan fazla olan Instagram ve Facebook gibi yurt dışı kaynaklı sosyal ağ sağlayıcıların adli veya idari makamlarca gönderilecek tebligat, bildirim veya taleplerin gereğinin yerine getirilmesi ve kişiler tarafından İnternet Kanunu kapsamında yapılacak başvuruların cevaplandırılması ve İnternet Kanunu kapsamındaki diğer yükümlülüklerin yerine getirilmesini temin için Türkiye’de en az bir kişiyi temsilci olarak atama, BTK’ya bildirme ve atadığı temsilciye ait iletişim bilgilerine internet sitesinde yer verme yükümlülüğü bulunmaktadır.

Sosyal ağ sağlayıcı, Türkiye’de yerleşik ve Türk vatandaşı gerçek bir kişiyi temsilci atayabileceği gibi dilerse Türkiye’de kurulmuş ve Türk mevzuatına göre tüzel kişilik kazanmış bir tüzel kişiyi de temsilci olarak atayabilmektedir. Türkiye’den günlük erişimi on milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcının temsilcisinin tüzel kişi olması halinde ise, bu temsilcinin doğrudan sosyal ağ sağlayıcı tarafından sermaye şirketi şeklinde kurulan bir şube olması gerekmektedir. Karar ile temsilcinin görevleri belirlenmiş ve temsilcinin BTK’ya bildirilme usulü açıklanmıştır.

Bahse konu yükümlülüklerle uyulmaması halinde, aşağıdaki yaptırımlar kademeli olarak uygulanmaktadır. İlk aşamada BTK tarafından temsilci atanması adına otuz gün süre verildiğine dair bildirimde bulunmaktadır.

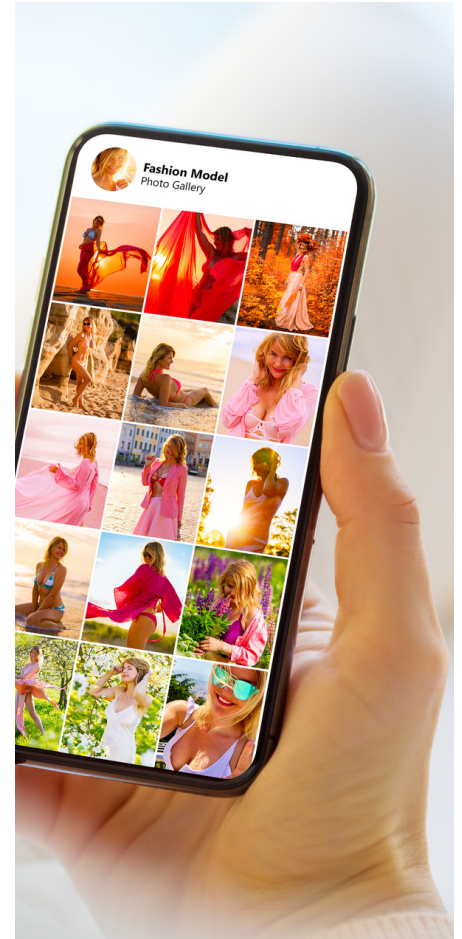


Bildirimi takiben otuz gün içinde yükümlülüğün yerine getirilmemesi halinde, on milyon TL ve bu idari para cezasının tebliğinden itibaren yine otuz gün içinde yükümlülüğün yerine getirilmemesi halinde, otuz milyon TL idari para cezası yaptırımı uygulanmaktadır. İkinci kez verilen idari para cezasının tebliğinden itibaren otuz gün içinde yükümlülüğün yerine getirilmemesi halinde ise, BTK tarafından Türkiye’de yerleşik vergi mükellefi gerçek ve tüzel kişilerin ilgili sosyal ağ sağlayıcıya reklam vermesi[1] ve bu kapsamda yeni sözleşme kurması yasaklanmaktadır. Aynı zamanda takip eden süreçlerde, internet trafiği bant genişliğinin %50 ile %90 arasında gittikçe artan oranlarda daraltılması söz konusu olabilecektir. Öte yandan, sosyal ağ sağlayıcı tarafından temsilci atama yükümlülüklerinin yerine getirilmesi durumunda verilen idari para cezalarının yalnızca 1/4’ü tahsil edilmektedir.

Belirtmekte fayda var ki, sosyal ağ sağlayıcıların temsilci tayin etmemesi durumunda öngörülen bu ağır yaptırımlar, özellikle bant genişliğinin yüzde doksana kadar sınırlandırılması, aslında sosyal medya platformlarının tamamen ulaşılamaz hale getirilmesi anlamına gelebilmektedir. Bu kadar ağır yaptırımın temsilci atama şartına bağlanmasının amacı, sosyal medya sağlayıcıları üzerinde baskı oluşturmak, istenmeyen içeriklerin hızla kaldırılmasını sağlamak ve muhalif içerik üreten anonim hesapların IP ve benzeri kimlik tanımlama bilgilerini elde etmeye çalışmaktır. Ayrıca, temsilci atanması durumunda bu bilgilerin BTK’ya iletilme olasılığı, bu platformları kullananlar tarafından öngörülebileceğinden, bu düzenleme oto sansüre yol açma potansiyeli taşımaktadır[1].

Kişiler Tarafından Yapılan Başvuruların Cevaplandırılması ve Sürecin Kolaylaştırılması

İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakkının veya özel hayat gizliliğinin ihlal edildiğini iddia eden kişilerin ilgili mercilere başvurarak içeriğin çıkartılması veya erişimin engellenmesi talebinde bulunma hakları vardır. Türkiye’den günlük erişimi bir milyondan fazla olan yurtiçi veya yurtdışı kaynaklı sosyal ağ sağlayıcının, bahse konu haklarının ihlal edildiğini (İnternet Kanunu madde 9 ve 9/A) iddia eden başvurucuya en geç kırk sekiz saat içerisinde olumlu ya da gerekçesi belirterek olumsuz cevap vermesi gerekmektedir. Ek olarak, sosyal ağ sağlayıcının kullanıcıların başvurularının alınmasını kolaylaştırması, bu amaçla kişilerin başvurularını Türkçe yapabilmelerine olanak tanınması ve Türkçe yapılan başvuruları yine Türkçe yanıtlaması gerekmektedir. BTK, başvurucunun şikâyeti üzerine sosyal ağ sağlayıcının başvuruları cevaplama yükümlülüğünü yerine getirip getirmediğini, altı aylık raporlama dönemlerinde toplu şekilde incelemektedir. Yapılan başvuruların cevaplanmasına yönelik yükümlülüklerin yerine getirilmemesi durumunda sosyal ağ sağlayıcı hakkında beş milyon TL idari para cezası yaptırımı uygulanmaktadır.



Adli Mercilere Bilgi Verilmesi

Türk Ceza Kanunu'nda ("TCK") çocukların cinsel istismarına yönelik suçlara (TCK madde 103), devlet sırlarına karşı suçlara ve casusluk (TCK madde 328, 329, 330, 331, 333, 334, 335, 336, ve 337), devletin birliğini ve ülke bütünlüğünü bozma (TCK madde 302), halkı yanıltıcı bilgiyi alenen yayma (TCK madde 217/A) ve anayasal düzene ve bu düzenin işleyişine karşı suçlara (TCK madde 309, 311, 312, 313, 314, 315 ve 316) konu internet içeriklerini oluşturan kişi veya faillere ulaşma amacıyla savcılık veya mahkemeler tarafından talep edilen bilgilere sosyal ağ sağlayıcının yanıt verme yükümlülüğü getirilmiştir. Aksi takdirde, Cumhuriyet Savcılığı veya mahkeme tarafından sosyal ağ sağlayıcı hakkında internet bant trafiği genişliğinin %90 oranında daraltılması için Ankara Sulh Ceza Hakimliği'ne başvurulabilmektedir. İnternet bant genişliğinin daraltılması kararı verilmesi halinde, karar öncelikle BTK'ya ve BTK tarafından da erişim sağlayıcılara bildirilmektedir. Erişim sağlayıcılar, daraltma kararını derhal ve en geç dört saat içinde yerine getirmektedir. Öte yandan, sosyal ağ sağlayıcının kullanıcı veri/bilgi talebini yerine getirmesi halinde, internet bant genişliğinin daraltılmasına ilişkin verilen karar iptal edilmektedir.

Raporlama Yükümlülüğü

Türkiye'den günlük erişimi 1 milyondan fazla olan yurtiçi veya yurtdışı kaynaklı sosyal ağ sağlayıcının, içeriğin çıkartılması ve/veya erişimin engellenmesine yönelik kararlar ve bunların uygulanmasına yönelik kendisine yapılan bildirimler ile kişiler tarafından kendisine yapılan başvurular hakkında BTK'ya altı aylık dönemler ile Türkçe dilinde düzenli olarak istatistiksel ve kategorik bilgi içeren rapor sunma yükümlülüğü bulunmaktadır. 1 Ocak – 30 Haziran dönemini kapsayan raporların temmuz ayı içinde, 1 Temmuz – 31 Aralık dönemini kapsayan raporların ise ocak ayı içinde BTK'ya gönderilmesi gerekmektedir. Ayrıca, sosyal ağ sağlayıcı; internet ortamında yapılan yayın içeriği nedeniyle kişilik hakkı veya özel hayatının gizliliği hakkına yönelik ihlal taleplerine ilişkin hazırladığı raporu, kişisel verilerden arındırılmış olarak internet sitesinde yayımlamak zorundadır. Raporlama yükümlülüğünün yerine getirilmemesi halinde, on milyon TL idari para cezası yaptırımını uygulanmaktadır.

Reklam Kütüphanesi Oluşturma Yükümlülüğü

Türkiye'den günlük erişimi bir milyondan fazla olan yurtiçi veya yurtdışı kaynaklı sosyal ağ sağlayıcıların; reklamın içeriği, reklam türü, reklam veren, reklamın yayında kaldığı dönem, reklamın hedef kitlesi ve reklamın hedef kitlesinin belirlenmesinde kullanılan parametreler, reklamın ulaştığı kişi ve grup sayısı gibi bilgileri içeren reklam kütüphanesi oluşturma ve altı aylık raporlarında buna ilişkin bilgilere yer verme yükümlülüğü bulunmaktadır. Ayrıca, sosyal ağ sağlayıcının, reklam kütüphanesine internet sitesinde kolayca görülebilecek ve doğrudan erişilebilecek şekilde yer vermesi gerekmektedir. Aksi takdirde, on milyon TL idari para cezası yaptırımını uygulanabilmektedir.

Başvuru Mekanizması Kurulması

Sosyal ağ sağlayıcılar, başlık etiketleri ve öne çıkarılan içeriklerin uyarı yöntemiyle kaldırılması amacıyla BTK ile işbirliği içinde etkin bir başvuru mekanizması kurmakla ve bu mekanizma hakkında, altı aylık raporların bir parçası olarak, BTK'ya bildirmekle yükümlüdür.

İçeriğin Çıkarılması ve Erişim Engellenmesi Kararlarının Uygulanması

BTK başkanı tarafından internet ortamında yapılan ve içeriği yine İnternet Kanunu'nda düzenlenen suçları oluşturduğu hususunda yeterli şüphe bulunan yayınlar hakkında içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilmektedir. Bu kararları yerine getirmeyen sosyal ağ sağlayıcıları hakkında bir milyon TL idari para cezası yaptırımını uygulanabilmektedir. Ek olarak; bu yönde verilen kararının yerine getirilmemesi durumunda, BTK tarafından sosyal ağ sağlayıcıya Türkiye'de yerleşik vergi mükellefi olan kişiler tarafından altı aya kadar reklam verilmesinin yasaklanmasına karar verilebilmekte ve sosyal ağ sağlayıcının internet trafiği bant genişliğinin %50 ile %90 arasında gittikçe artan oranlarda daraltılması adına gerekli prosedür yürütülebilmektedir. Ayrıca sosyal ağ sağlayıcı, yirmi dört saat içerisinde hukuka aykırı içeriği çıkarma veya erişimin engellenmesi kararına uymamasından kaynaklanan zararların tazmin edilmesinden sorumlu olmakta ve bu hukuki sorumluluğun yerine getirilmesi için ayrı bir dava açılmış olması gerekmektedir. Sosyal ağ sağlayıcı, kararın tebliğinden itibaren hukuka aykırı içeriği derhal ve en geç 4 saat içinde kaldırmazsa, başlık etiketleri veya öne çıkarılan içerik yoluyla işlenen suçlardan doğrudan sorumlu tutulmaktadır.

Mevcut uygulama yukarıda belirtildiği gibi olmakla beraber, Anayasa Mahkemesi, 11/10/2023 tarihli ve 2020/76 E. ve 2023/172 K. sayılı kararında[1]; İnternet Kanunu'nun BTK Başkanı'na resen erişimin engellenmesi yetkisi veren hükümleri ile internet ortamındaki yayınlara, erişim engeli ya da içeriğin çıkarılması kararı verilmesini öngören maddeleri Anayasa'ya aykırılık gerekçesi ile iptal etmiştir. İptal kararı; Resmi Gazete'de yayımlanmasından dokuz ay sonra, yani 10.10.2024 tarihinde yürürlüğe girecektir. Anayasa'nın 38. maddesi, suç şüphesi altındaki kişiye karşı tedbir alınmasını kesin olarak yasaklamamakla birlikte, bu tedbirlerin ceza yargılaması süreciyle ilişkili ve geçici olması gerektiğini belirtir. Dolayısıyla AYM kararında, ceza kanunlarında suç olarak düzenlenen eylemlerin işlendiğinin henüz kesinleşmiş bir mahkeme kararıyla tespit edilmeden, BTK tarafından yapılacak suç tespitine bağlı olarak nihai bir tedbir mahiyetinde olan içeriğin çıkarılması kararı verilmesinin ve bu kararın icra edilmemesi durumunda idari para cezası uygulanmasının masumiyet karinesini ihlal ettiği değerlendirilmiştir.

Kullanıcı Haklarının Korunması, Verilerin Türkiye’de Barındırılması Yükümlülüğü, Can ve Mal Güvenliğinin Korunması, Kriz Planı Oluşturulması, BTK’ya Bilgi Verilmesi ve Çocuklara Özgü Ayırıştırılmış Hizmet Sunulması

Kullanıcı haklarının korunmasına ilişkin yükümlülükleri kapsamında sosyal hizmet sağlayıcı; kullanıcılar arasında eşit ve tarafsız davranmakla, kullanıcılara önerdiği içeriklere ilişkin tercihleri güncelleme ve kişisel verilerin kullanılmasını sınırlandırma seçeneği sunmakla, Türkiye’den erişen kullanıcıları etkileyen kullanıcı hesaplarına ilişkin önemli güvenlik ihlallerinin tespitinden itibaren en geç yetmiş iki saat içerisinde BTK’ya ve kullanıcıları Türkçe dilinde bilgilendirmekle, kullanıcı haklarını etki eden güncellemelere kullanıcıların kolayca ulaşabilmesini sağlamakla, kullanıcılara öneriler sunarken hangi parametreleri kullandığını açık ve kolaylıkla ulaşılabilir şekilde internet sitesinde yer vermekle, başkasını taklit eden veya ele geçirilen hesaplara yönelik Türkçe, açık ve kolaylıkla ulaşılabilir bir başvuru mekanizmasını kurmakla ve başvuruları makul sürede sonuçlandırmakla yükümlüdür.



Türkiye’den günlük erişimi bir milyondan fazla olan yurtiçi veya yurtdışı sosyal ağ sağlayıcıların, Türkiye’deki kullanıcıların verilerini Türkiye’de barındırma yönünde gerekli önlemleri alma yükümlülüğü bulunmaktadır. Sosyal ağ sağlayıcı; (i) gecikmesinde sakınca bulunan hallerde, kişilerin can ve mal güvenliğini tehlikeye sokan içeriklere ilişkin her türlü bilgiyi derhal kolluk birimlerine bildirmekle, (ii) kamu güvenliğini/kamu sağlığını etkileyen olağanüstü durumlara ilişkin kriz planı oluşturmakla ve bahse konu planı BTK’ya bildirmekle, (iii) BTK tarafından kurumsal yapı, bilişim sistemleri, algoritmalar, veri işleme mekanizmaları ve ticari tutumlar da dahil olmak üzere talep edilen bilgileri en geç üç ay içerisinde BTK’ya bildirmekle, (iv) çocuklara özgü ayırıştırılmış hizmet sunarak bu konuda gerekli tedbirleri almakla yükümlüdür.

Bu alt başlık ile belirtilmiş yükümlülüklerin yerine getirilmemesi halinde, sosyal ağ sağlayıcıya bir önceki takvim yılındaki küresel cirosunun %3’üne kadar idari para cezası yaptırımını uygulanmaktadır.

İdari Para Cezası Yaptırımlarının Ödenmemesi, Reklam Yasağı ve Yerinde İnceleme

Sosyal ağ sağlayıcının, idari para cezalarını bir yıl içerisinde birden fazla kez süresinde ödememesi durumunda, sosyal ağ sağlayıcıya altı aya kadar Türkiye’de yerleşik vergi mükellefi olan kişiler bakımından reklam verme ve bu kapsamda yeni sözleşme kurma yasağı uygulanabilmektedir. Ek olarak, reklam yasağı boyunca sosyal ağ sağlayıcıya para transferi yapılması da yasaklanmaktadır. Reklam yasağına aykırı davranan Türkiye’de yerleşik vergi mükelleflerine on bin TL ile yüz bin TL arasında idari para cezası yaptırımı uygulanabilmektedir. Belirtmek gerekir ki, yukarıda belirtilmiş olan idari para cezaları önceki yılın yeniden değerlendirme oranlarına göre arttırılmaktadır. Ayrıca, BTK, İnternet Kanunu’na ve Karar’a uygun davranılıp davranılmadığının tespiti adına sosyal ağ sağlayıcının tesislerinde yerinde inceleme yapma yetkisine sahiptir.

Sonuç olarak, İnternet Kanunu ve Karar, sosyal ağ sağlayıcıların yükümlülüklerine ilişkin yol gösterici ve detaylı hükümler içermekle beraber bu platformları yoğun bir denetime tabi tutmaktadır. Bu nedenle sosyal ağ sağlayıcıların yükümlülüklerini yerine getirirken yine İnternet Kanunu ve Karar’da yer alan gereklilikleri ve usulleri dikkate alması gerekmektedir. Nitekim kademeli olarak arttırılan yaptırımlar sosyal ağ sağlayıcılar bakımından büyük bir yük oluştururken reklam yasağı ve internet trafiği bant genişliğinin daraltılması gibi yaptırımlar sosyal ağları işlemez hale getirebilmektedir. Nitekim bazı sosyal ağ sağlayıcı şirketler de kanunun yapımı aşamasında katıldıkları meclis alt komisyon çalışmalarında buna ilişkin çekincelerini ifade etmişlerdir[1]. Belirtmek gerekir ki, sosyal ağ kullanımının artışıyla beraber sosyal ağlar üzerinde gerçekleştirilen hak ve ihlallerin ve işlenen suçların giderek arttığı göz önünde bulundurulduğunda; kişilik hakları ihlal edilen kişiler tarafından haklarının kullanılmasına hizmet edecek hükümler oldukça önemlidir.

Av. Benay ÇAYLAK

Dijital Hizmetler Yasası Uyum Sürecine İlişkin Gelişmeler

Avrupa Komisyonu (European Commission) ("Komisyon") 1 Aralık 2023'te sosyal medya, uygulama mağazaları veya pazaryerleri gibi çevrimiçi platformlara odaklanarak dijital hizmetlerin hüküm ve koşullarını içeren Dijital Hizmetler Hüküm ve Koşullar Veri Tabanı'nı (Digital Services Terms and Conditions Database) ("Veri Tabanı") duyurdu.

Bu Veri Tabanı, çevrimiçi platformların, hüküm ve koşullarının kolayca anlaşılabilir, sade bir dilde olan özetlerini iş yaptıkları Avrupa Birliği ("AB") üye ülkelerin dillerinde sunma yükümlülüğü de dahil olmak üzere, Dijital Hizmetler Yasası (*Digital Services Act*) ("DHY") tarafından ilk kez ortaya konan muhtelif şeffaflık gereksinimlerini tamamlayan bir Komisyon girişimidir. DHY; 17 Şubat 2024'ten itibaren çevrimiçi pazar yerleri, web barındırma hizmetleri, bulut hizmetleri, arama motorları ve sosyal medya platformları da dahil olmak üzere AB'de sunulan çok çeşitli aracı hizmetlere uygulanmaya başlayacağından bu hizmet sağlayıcıların belirli bilgileri mevcut hüküm ve koşullarına dahil etmelerini gerektirecektir. Bu noktada Veri Tabanı, DHY uyum sürecinde önem arz etmektedir.

Veri Tabanı, kullanıcılar, düzenleyiciler ve paydaşlar için başvurulabilecek bir kaynak görevi görecek. Düzenleyiciler, dijital manzarayı gözlemleyebilecek ve regülasyonlara hukuken uyumu değerlendirebilecek; araştırmacılar ise değişen hüküm ve koşullara ilişkin olarak Veri Tabanı üzerinden gerçek zamanlı bir şekilde fikir sahibi olma fırsatını yakalayacaktır.



Veri Tabanı, Komisyon'un yeni nesil internet programının desteğiyle, Fransa'nın dijital işler elçisinin politik sponsoru olduğu bir girişim olan Açık Terimler Arşivi (Open Terms Archive) ("ATA") tarafından geliştirilen açık kaynaklı bir yazılımı kullanmaktadır. ATA, dijital hizmet şartlarının her versiyonunu kamuya açık ve ücretsiz olarak erişime sunmaktadır. Yeni piyasaya sürülen Veri Tabanı, şu an itibarıyla halihazırda muhtelif hizmet sağlayıcılardan 790 tane hüküm ve koşulları havuzunda bulundurmakta; Veri Tabanındaki hüküm ve koşulları her gün defalarca dikkatle inceleyen ve yeni değişikliklere dikkat çeken bir otomatikleştirilmiş sistem kullanmaktadır.

DHY, muhtelif şeffaflık mekanizmaları vasıtasıyla, tamamen yeni bir hesap verebilirlik düzeyini ilk kez ortaya koymaktadır. Tüm çevrimiçi platformların aylık aktif kullanıcılarını açıklama ve şeffaflık raporları yayınlama gerekliliği ile belirlenmiş çok büyük çevrimiçi platformlar veya arama motorlarının reklam havuzlarını tanıtmaya, denetim raporları yayınlama, risk değerlendirme raporları oluşturma ve araştırmacı erişimi sağlama gerekliliği de buna dahildir. DHY ayrıca, Komisyon'a, platformlarda içerikler kaldırıldığı veya sınırlandırıldığı zaman kullanıcılara sunması gereken bilgileri detaylandıran sebep beyanlarını içeren bir Şeffaflık Veri Tabanı'nı devamlı olarak tutmayı şart koşmaktadır.

Komisyon, 18 Aralık 2023 tarihinde X'in (eski adıyla Twitter) risk yönetimi, içerik denetimi, karanlık desenler, reklam şeffaflığı ve araştırmacılar için veri erişimi ile bağlantılı alanlarda DHY kapsamında herhangi bir ihlalinin olup olmadığını değerlendirmek amacıyla X'e karşı resmi ihlal davası açtığını duyurdu.

Komisyon, 18 Ocak 2024'te DHY kapsamında çok büyük çevrimiçi platformlar ve arama motorlarının 17'sinden (AliExpress, Amazon Store, AppStore, Bing, Booking.com, Facebook, Google Arama, Google Play, Google Haritalar, Google Alışveriş, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, YouTube ve Zalando) bilgi talep ettiğini duyurdu. Bu duyuru ile uygun araştırmacılara çevrimiçi arayüzlerinde kamuya açık olan verilere gereksiz gecikme olmaksızın erişim sağlama yükümlülüğüne uymak için aldıkları önlemler hakkında daha fazla bilgi sağlamalarının talep edildiği açıklandı. Komisyon, 8 Şubat 2024 tarihine kadar bu bilgilerin sunulması gerekliliğini de belirtti.

Veri Tabanı, yalnızca kullanıcılara fayda sağlamakla kalmayacak olup aynı zamanda yeni geliştirilecek dijital hizmetlere rehberlik etme ve mevcut hizmet sunan şirketler dahil olmak üzere dijital alanda faaliyet gösteren bütün aktörlerin birbirlerinden öğrenebilecekleri başarılı uygulamaları bir araya getirme açısından önemlidir. Komisyon'un Veri Tabanı ve X'e karşı resmi işlem başlattığına ilişkin duyuruları ile Komisyon'un çok büyük çevrimiçi platformlar ve arama motorlarından bilgi talep etmesi DHY uyum sürecinin ivme kazandığını ortaya koymaktadır. Komisyon'un veri erişimi ile ilgili yükümlülüklerin ihlal edildiği şüphesi de olduğundan ve elbette DHY AB'deki çevrimiçi içeriği ve iş uygulamalarını düzenler ve çoğu sağlayıcı için 17 Şubat 2024'ten itibaren yürürlüğe gireceğinden çalışmaların önümüzdeki dönemde de artacağı düşünülmektedir.

AVRUPA BİRLİĞİ VERİ YASASI

AV. İLYAS ÇETİNKAYA

Avrupa Birliği Konseyi (Council of the European Union) ("AB Konseyi"), Avrupa Parlamentosu'nun (European Parliament) 9 Kasım 2023'te onaylamasının ardından 27 Kasım 2023'te Veri Yasası'nın (Data Act) nihai halinin kabul edildiğini duyurdu. Bu önemli mevzuat, dijital ekonomide verilerden üretilen değer in adil dağılımını yeniden şekillendirmeyi amaçlıyor. Aynı zamanda Veri Yasası kamu hizmetlerinin niteliksel ve niceliksel yönden iyileştirilmesi, doğal afet ve benzeri olağanüstü durumlarda kamusal müdahalelerin daha etkin yapılabilmesi için veriye erişimin ve veri kullanımının kolaylaştırılmasını da amaçlamaktadır.

AB Konseyi'nin Veri Yasası ile ulaşmak istediği amacı daha iyi anlayabilmek için dijital çağın ve bilgi toplumunun ekonomisine ilişkin birtakım temel kavramları bilmekte yarar vardır. Şöyle ki;

1

Bilgi Ekonomisi

Bir ürünün ya da hizmetin ortaya çıkabilmesi için gereken temel unsurun yani üretim faktörünün bilgi olduğu bir ekonomik modeldir. Yazılım ve Bilgi Teknolojileri ("BT") sektörü, uzmanlık, bilgi ve deneyim gerektiren hukuk, danışmanlık gibi profesyonel hizmetler bilgi ekonomisine örnek gösterilebilir. Facebook, X, Instagram gibi sosyal medya platformları da bilgi ekonomisinin en bilinen örnekleridir. Bilgi ekonomisi, mal ve hizmet üretiminde araştırma geliştirme ve üretim geliştirme süreçlerinde bilginin temel unsur olarak kullanılmasını ifade eder. Hedef pazarda değişen satın alma davranışlarına veya müşterilerin yeni gereksinimlerine göre teknolojik bir ev aletine yeni özellikler eklenmesi de bilgi ekonomisinin bir örneğidir. Bu örnekte satın alma davranışlarının nasıl bir değişikliğe uğradığına ya da müşteri gereksinimlerinin ne yönde farklılaştığına dair verilerin elde edilmesi ve çözümlenmesi ile kazanılan bilgi, AR-GE sürecinin temel dayanağıdır.

2

Dijital Pazarlama ve Veri Analitiği

Bilgi ekonomisinin temel uğraş alanlarından biridir. Dijital Pazarlama ve Veri Analitiği, müşteri davranışları değerlendirilerek dijital pazarlama stratejilerinin oluşturulması konusunda veri çözümlenmesi yapılmaktadır.

Bu temel kavramlardan hareketle, veriye adil erişimin sağlanması ticari rekabeti artıracaktır. Ticari rekabetin artması ise hem ürün ve hizmet kalitesini artırır hem de girişimciliği destekleyecektir. İşletmelerin ve ulusal ekonominin başarısı, bilginin üretilmesinin yanı sıra bilginin ele geçirilmesi, içselleştirilmesi ve etkin bir şekilde kullanılabilmesine bağlıdır. Veri Yasası'nın temel amacı da budur.

Veri Yasası, hizmet sağlayıcıların ve ürün üreticilerinin, kullanıcıların hizmetlerindeki verilere erişmesine ve bunları yeniden kullanmasına izin vermesini zorunlu kılar. Buna, verilerin üçüncü taraflarla paylaşılması ve tüm ekonomik sektörlerde veri taşınabilirliğinin artırılması da dahildir. Bireyler ve işletmeler için daha fazla kontrole vurgu yaparak hem kişisel hem de kişisel olmayan veriler için geçerlidir.

Temel hedeflerden biri rekabetçi bir veri pazarını teşvik etmektir. Verilere erişimi kolaylaştırarak inovasyona yeni kapılar açar ve adil, makul ve ayrımcı olmayan veri paylaşım uygulamaları sağlar. Veri Yasası, ürün verileri ile ilgili hizmet verileri arasında ayırım yaparak ticari sırlar ve fikri mülkiyet hakları için güçlü bir koruma sağlar.

Veri Yasası; ticari sırların ve fikri mülkiyet haklarının yeterli düzeyde korunmasını ve olası suistimal edici davranışlara karşı gerekli önlemlerin alınmasını sağlıyor. Yeni düzenleme, veri paylaşımını teşvik ederken, AB endüstrisini desteklemeyi, aynı zamanda istisnai durumlara karşı koruma sağlamayı ve anlaşmazlıkların çözümü için mekanizmalar sağlamayı amaçlıyor.

Nesnelerin interneti (Internet of things) ("IoT"), fiziksel nesnelerin internet ağı üzerinden birbirileri ile veya internete bağlı cihazlarla iletişim kurma yeteneğini ifade eden bir kavramdır. Bu nesneler, sensörler, yazılımlar ve diğer teknolojiler aracılığıyla veri toplayabilir, paylaşabilir ve işleyebilirler. Uzaktan açılabilen ekmek kızartma makinesi dünyanın ilk internet kontrollü cihazıdır.[1] Akıllı ev teknolojileri de bu duruma örnektir. Akıllı fabrika sistemleri de nesnelerin internetini kullanarak üretim süreçlerini geliştirir ve verimliliği artırır. IoT konseptinin hayatımıza girişi 1990'ların başında Massachusetts Teknoloji Enstitüsü (Massachusetts Institute of Technology) ("MIT") laboratuvarlarında önerilmiştir.

3

Dijital Ekonomi

Dijital Ekonomi ise e-ticaret, dijital platformlarda içerik üretimi ve internet üzerinden verilen hizmetler gibi ekonomik faaliyetlerde bilgi ve iletişim teknolojilerinin kullanılmasını ifade eden bir kavramdır.

IoT, eğer bir kamusal iletişim ağına bağlı ise Veri Yasası kapsamında bir terminal ekipmanı olarak kabul edilmiştir. Terminal ekipmanı, kısaca BT alanında kullanılan, veri işlenen veya saklanan cihaz demektir. Dolayısıyla Veri Yasası, IoT uygulamalarında toplanan veriye erişim ve bunun kullanımını da kapsamaktadır.

Veri Yasası ile tüketicilerin bir bulut sağlayıcısından diğerine kolayca geçmesine olanak tanındı. Veri paylaşımı ve işlemeye yönelik birlikte çalışabilirlik standartlarının yanı sıra, yasa dışı veri aktarımlarına karşı da önlemler getirildi. Ayrıca Veri Yasası'ndan bazı cihazların satış sonrası hizmetlerinin daha ucuz ve verimli hale getirilmesi beklenmektedir.

Türkiye'de Türk şirketlerin uluslararası rekabet gücünün artırılması, start-up girişimlerin çoğalması ve büyümesi, kullanıcıların ve devletin uygun amaç doğrultusunda veriye erişimi konusunda yükümlülüklerin, yetki ve hakların belirlendiği, sadece bilgi ekonomisine ilişkin veri üzerine yoğunlaşan, Veri Yasası'na benzer bir yasal düzenlemeye gereksinim olduğu kanaati ağır basmaktadır.

PHISHING SALDIRILARI

Av. Onur ALAS

PHISHING (Oltalama) Nedir?

Phishing, kötü niyetli kişilerin e-posta, SMS veya telefon gibi elektronik iletişim araçları ile bir kuruluş veya güvenilir bir hizmet sağlayıcısını taklit ederek, kullanıcıların kişisel bilgilerini çalmak veya hassas bilgilere erişmek için kullandığı bir sosyal mühendislik saldırısıdır.

E-POSTA PHİSHİNG'İ

Tehdit aktörleri meslektaş, tanıdık veya saygın kuruluşlar gibi davranarak hassas bilgiler ister veya kurbanları kötü amaçlı yazılım indirmeye ve çalıştırmaya teşvik eder. Yem genellikle kullanıcıyı e-postayı açmaya teşvik eden konu satırına sahip bir e-postadan oluşur; örneğin konu satırında bir uyarı, bir eylem veya bilgi talebi bulunur.



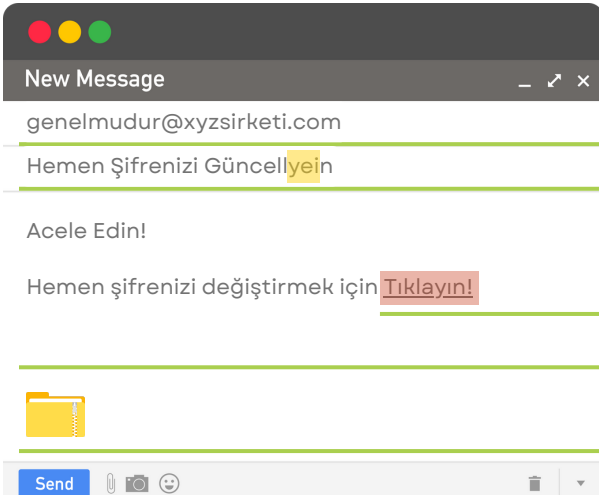
Finansal güvenlik uyarıları ve güncellemeler



Kuruluş çapında duyurular ve güncellemeler



Kullanıcıya özel uyarılar



Nasıl Korunurum?

Gönderici adresini mutlaka kontrol edin
Başlık ve içerikte yazım hataları olması

Güvensiz linklere tıklamaktan kaçının

Risk veya kazanç konusunda aciliyet duygusu yaratan maillere şüphe ile yaklaşın

Güvensiz mail eklerini bilgisayarınıza indirmeyin

PHISHING SALDIRILARI

Av. Onur ALAS

SESLİ PHİSHİNG

Sesli phishing (Vishing) tekniğinde, dolandırıcılar telefon aramaları veya sesli mesajlar kullanarak kişisel bilgileri çalmaya çalışır. Genellikle, dolandırıcılar banka gibi güvenilir bir kuruluşu taklit eder ve hedeflerden hassas bilgileri veya şifreleri talep eder. Bu bilgiler daha sonra dolandırıcılar tarafından hedefin mali kaynaklarına erişmek veya kimlik hırsızlığı yapmak için kullanılır.

KAMPANYALI TEKLİFLER

Saldırganlar size kampanyalı bir teklif sunabilir, teklifi kabul edip başvuru yapmak istediğinizde bilgilerinizi talep edebilir.



KİŞİSEL VERİLERİNİZ

Saldırganlar kendilerini banka personeli gibi tanıtarak **güvenlik sorusu cevabınızı, kartınızın son 3 hanesi** gibi kişisel verilerinizi sizden teyit alma aldatmacasıyla talep edebilir.

HESABINIZ TEHLİKEDE!

Saldırganlar size banka hesabınızın tehlikede olduğunu ve acilen önlem alınması gerektiği söyleyerek sizi panik içine sürüklemeye çalışır. Karşı tarafın telaş içinde olmasından faydalanabilir.

AYNI ANDA BAĞLANTI

Saldırganlar aynı anda sizi taklit ederek banka ile iletişim halinde olabilir. Sizin adınıza internet şubesinden 'şifre sıfırlama' işlemi yaparak, cep telefonunuza gelen güvenlik kodunu talep edebilir.



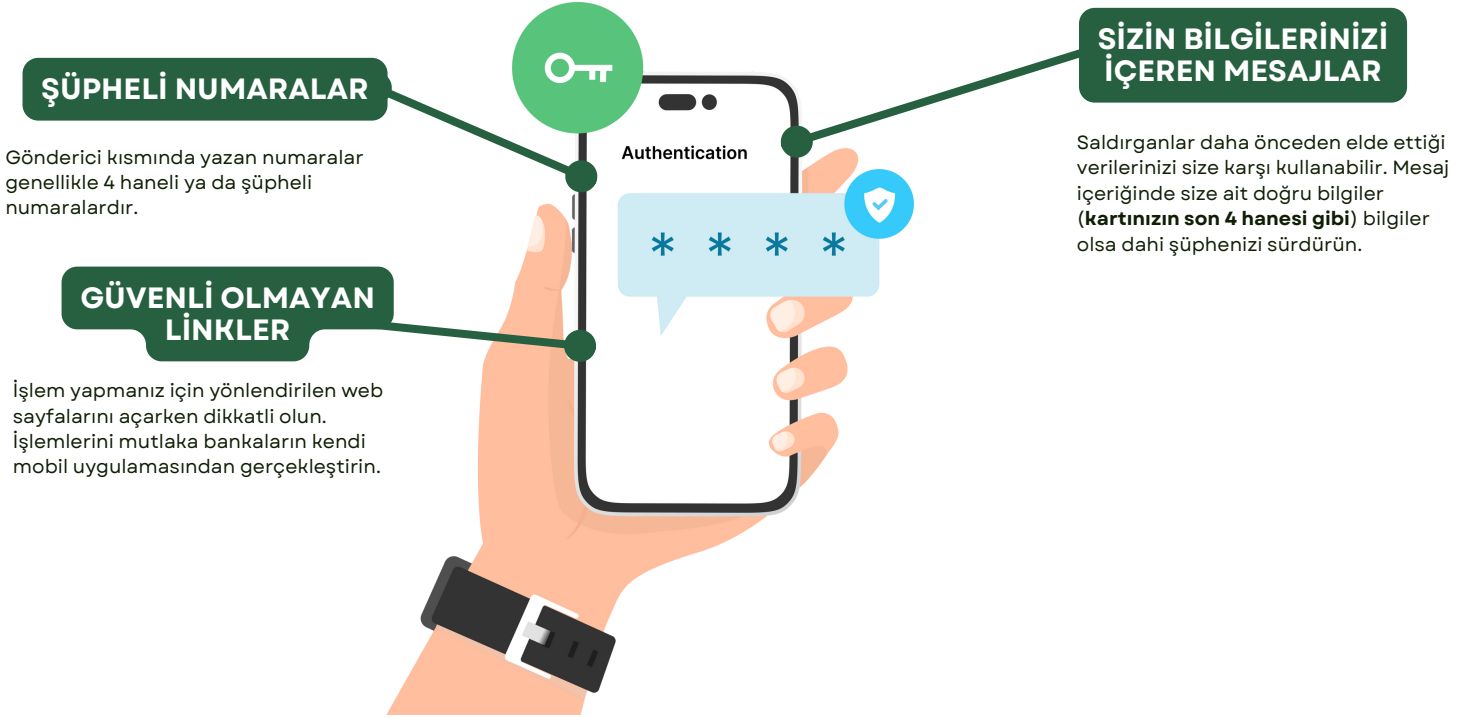
2021'de Amerika'da 59,4 Milyonun Üzerinde İnsan Vishing Kurbanı Oldu

2021'de 59,49 milyondan fazla Amerikalı (%23) vishing nedeniyle para kaybetti. Üstelik bu sayı 2020'de 56 milyon (%22) ve 2019'da 43 milyondur.

Kaynak: [2020 Internet Crime Report](#)

SMS PHİSHİNG

Bu yöntemde, dolandırıcılar güvenilir bir kuruluşun kimliğine bürünerek sahte mesajlar gönderirler. Bu mesajlar genellikle **acil eylem gerektiren** bir durum yaratır ve kullanıcıları kişisel bilgilerini, örneğin banka hesap detaylarını veya şifrelerini paylaşmaya teşvik eder.



SOSYAL MEDYA PHİSHİNG'İ

Dolandırıcıların sosyal medya platformlarını kullanarak kişisel bilgileri çalmaya çalıştığı bir dolandırıcılık türüdür. Bu durumda, dolandırıcılar genellikle sahte hesaplar oluşturur ve güvenilir bir kişi veya kuruluş gibi davranır. Dolandırıcılar, hedeflerini özel mesajlar veya sahte promosyonlar yoluyla kişisel bilgilerini paylaşmaya teşvik eder.





Kaynakça

Sızma Testleri ve Ceza Hukuku - Av. Celil Aktaş

[1] IBM, "What is penetration testing?", <https://www.ibm.com/topics/penetration-testing> Erişim Tarihi: 24.01.2024

[2] YİĞİT, Tuncay / AKYILDIZ, Muhammed Alparıslan, Sızma Testleri İin Bir Model Ađ Üzerinde Siber Saldırı Senaryolarının Deđerlendirilmesi, "Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi", Cilt:18, Sayı:1, 2014, (ss.14-21), s.14.

[3] ÇETİN, Muhammet Sefa, Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu (TCK m. 243), "Türkiye Adalet Akademisi Dergisi", Yıl: 12, Sayı: 45, Ocak 2021, (ss.1-28), s. 9.

[4] KARAKEHYA, Hakan, Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu, "Türkiye Barolar Birliđi Dergisi", Sayı: 81, 2009, (ss. 1-24), s. 16.

[5] İstanbul Bilgi Üniversitesi IT Bilişim Teknolojileri, "DDoS (Dađıtık Hizmet Engelleme)", <https://www.https://it.bilgi.edu.tr/tr/guvenlik/ddos/> Erişim Tarihi: 26.01.2024

[6] ERMEYDAN, Damla, "Türk Ceza Kanununda Bilişim Suçları", Seçkin, 2. Baskı, Ankara, 2023, s. 120-121.

[7] YILMAZ, Sacit, 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, "Türkiye Barolar Birliđi Dergisi", Sayı: 92, 2011, (ss. 62-100), s. 79.

[8] SINAR, Hasan, Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK md. 136), "Kişisel Verileri Koruma Dergisi", 2(1), 2020, (ss. 33-62), s. 52.

Sosyal Ağ Sağlayıcılarının Hukuki Sorumluluğu - Av. Merve Aslan

[1] Anayasa Mahkemesi (AYM). K.2023/172. (11.10.2023) :

<https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2023/172> . Erişim Tarihi:
12.01.2024.

[2] Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (Kanun No. 7418). Resmi Gazete 31987 (18.10.2022).

[3] Dülger, M. V. (2023). Sosyal Ağ Sağlayıcıların İnternet Haber Sitelerinin Ve Şebekeler Üstü Hizmet Sağlayıcıların Hukuki Relimi Ve Eleştirisi.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4425002 . Erişim Tarihi:
01.01.2024.

[4] İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (Kanun No. 5651). Resmi Gazete 26530 (23.05.2007).

[5] İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun (Kanun No. 7253). Resmi Gazete 31202 (31.07.2020). Erişim Tarihi: 12.01.2024

[6] TBMM, Yasama Dönemi 27, Yasama Yılı 5, Sıra Sayısı 340 :

<https://www5.tbmm.gov.tr/sirasayi/donem27/yil01/ss340.pdf> .

[7] Temsilci Belirleme ve Bildirme Yükümlülüğünü Yerine Getirmeyen Pinterest Inc. Adlı Sosyal Ağ Sağlayıcıya Reklam Verilmesinin Yasaklanmasına İlişkin Başkan Kararı (Karar No. 3767). Resmi Gazete 31369 (19.01.2020).

<https://www.resmigazete.gov.tr/ilanlar/eskiilanlar/2021/01/20210119-4-1.pdf> . Erişim Tarihi: 12.01.2024

[8] Temsilci Belirleme ve Bildirme Yükümlülüğünü Yerine Getirmeyen Twitter Inc. Adlı Sosyal Ağ Sağlayıcıya Reklam Verilmesinin Yasaklanmasına İlişkin Başkan Kararı (Karar No. 3768). Resmi Gazete 31369 (19.01.2020).

<https://www.resmigazete.gov.tr/ilanlar/eskiilanlar/2021/01/20210119-4-1.pdf> . Erişim Tarihi: 12.01.2024

[9] Temsilci Belirleme ve Bildirme Yükümlülüğünü Yerine Getirmeyen Twitter Inc. (Periscope/Scope) Adlı Sosyal Ağ Sağlayıcıya Reklam Verilmesinin Yasaklanmasına İlişkin Başkan Kararı (Karar No. 3769). Resmi Gazete 31369 (19.01.2020).

<https://www.resmigazete.gov.tr/ilanlar/eskiilanlar/2021/01/20210119-4-1.pdf> . Erişim Tarihi: 12.01.2024

Avrupa Birliği Veri Yasası - Av. İlyas Çetinkaya

[1] Süleyman Kevük, Bilgi Ekonomisi, Journal of Yasar University, 1(4), 2006, sayfa 322.

[2] Erdal Erdal/Atilla Ergüzen, Nesnelerin İnterneti (IoT), Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi, 2020, 12(3), sayfa 27.

[3] Erdal Erdal/Atilla Ergüzen, Nesnelerin İnterneti (IoT), Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi, 2020, 12(3), sayfa 27.



İstanbul Barosu
Bilişim Hukuku Komisyonu

DİJİTAL BÜLTEN

İki ayda bir yayımlanır.
Ocak - Şubat 2024
Sayı: 1

Yayından Sorumlu Yürütme Kurulu Üyeleri

Av. Fehmi Ünsal Özmestik
Av. Ecem Sağol

Yayın Ekibi

Av. Pınar Saruhan
Av. Mert Özyiğit
Av. Celil Aktaş
Av. Merve Aslan
Av. Benay Çaylak
Av. İlyas Çetinkaya
Av. Onur Alas
Av. Büşra Nur Aydın
Av. Gülce Demirel

Görseller & Tasarım

Av. Onur Alas



Şahkulu Mahallesi Serdar-ı Ekrem
Sokak No:7 Beyoğlu , İstanbul, Turkey



www.istanbulbarosu.org.tr